REMARKS

The present invention relates to a method for preventing unauthorized programs from spoofing data entry screens, such as password entry screens. The present invention employs authentication indicia that functions as a "reverse password" that is used by the computer to authenticate valid data entry screens. The presence or absence of the authentication data indicates to the user whether the data entry screen is valid. Because the authentication data is stored in a secure memory, it is not possible for a rogue program to spoof the data entry screen. Additional measures can be taken to inhibit execution of application programs, such as a video capture program, while the data entry screen is displayed.

Claims 1, 3, 5, 7 - 12, and 14, 15, 17, 18, and 20 have been amended. Claims 6, 13, 16 and 19 have been canceled. Two independent claims remain: claims 1 and 11. Claims 1 and 11 have been amended to incorporate the limitations of claim 6, which has been canceled. Thus, the previous rejection of claims 1 and 11 have been rendered moot by the amendment. The following arguments address the rejection of claim 6.

Claim 6 was rejected under 35 U.S.C. § 103 as being unpatentable over Windows NT. This rejection is improper. First, Windows NT does not display authentication indicia on data entry screens. In Windows NT, pressing Ctrl-Alt-Delete functions as a secure attention sequence (SAS) which initiates a secure log-on process. As part of the log-on process, Windows NT displays a password entry screen having fields for entering the user name and password. To gain access to the system, a user enters a user name and password, which serve to authenticate the user to the computer. If a valid user name and password is given, the operating system allows the user access to the system. The Examiner points out that Windows NT may display the user name of the last person that logged on in the user name field of the password entry screen. However, the user name is not authentication data as defined by the amended claims. As noted above, the authentication indicia recited in the claims comprises indicia used by the computer to authenticate valid data entry screens to the user. The authentication data recited in the claims functions as a reverse password. In contrast, the user name entered in the user name field of the NT log-on screen comprises data entered by the user to authenticate himself to the computer.

Second, the claimed invention temporarily halts the execution of programs not needed by the security module while the data entry screen is displayed, and restarts halted programs after the password entry screen is removed from the display. There is no evidence in the record to support the Examiner's bare assertion that Windows NT temporarily halts and then restarts execution of programs running when the log-on screen is displayed. On the contrary, Ozzie et al. (Patent No. 5,664,099) indicates that the secure attention sequence (Ctrl-Alt-Delete) "terminates any application programs which are in operation during the password entry sequence." Col. 1, lines 60-63.) There is nothing in the record indicating that Windows NT restarts halted programs after the password entry screen is displayed.

The remaining art cited by the Examiner also fails to teach or suggest temporarily halting programs while a data entry screen is displayed and then restarting the halted program when the data entry screen is removed from the display. The Examiner states that this element is implicit in Hatfield because the intention of the secure attention sequence (SAS) is to prevent spoofing. The Examiner's statement is inaccurate. The purpose of the SAS is to invoke the logon process, not to prevent spoofing. On the contrary, Hatfield itself warns against spoofing and offers that the best protection against spoofing is to "always maintain tight physical security." Nowhere does Hatfield teach or suggest halting executing programs and then restarting the programs when the data entry screen is removed. Pfleeger suggests terminating running process by giving a BREAK command or by turning off the computer. There is no teaching or suggestion to restart the halted process.

For reasons set forth above, Applicant believes that amended claims 1 and 11 define over the art made of record.

Claims 7-10 claim various techniques that can be used for "freezing" execution of programs while a data entry screen is displayed. The Examiner makes nothing more than a bare assertion that these techniques are old in the art. While similar techniques may have been used in the past to perform different purposes or functions, there is absolutely nothing in the record to suggest that the specific techniques recited by claims 7-10 have been used for the specific purposes recited in the claims. Applicant requests the Examiner to produce some authority or concrete evidence of the facts officially noticed by the Examiner. In the absence of concrete evidence, claims 7 – 10 should be allowed.

Applicant would greatly appreciate the opportunity to respond to any new evidence cited by the Examiner and requests that any action citing new evidence be non-Final.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

David Bennett

Dated: January 23, 2006

David E. Bennett
Registration No.: 32,194

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844